REMARKS

The Office Action mailed June 19, 2009 maintained the rejection of all pending claims 1-25, and made the rejections of the claims final. Applicants have amended claims, and are filing a request for continued examination (RCE). Specifically, Applicants have amended above claims 1, 13 and 22-25; and have canceled claims 3 and 16. As such, claims 1-2, 4-13, 15 and 17-25 are pending. Applicants request reconsideration in view of the amendments above and the following remarks.

Claim Rejections - 35 U.S.C. 103

Claims 1-13 and 15-25 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro (European Patent Application EP 0856821) in view of Barlow (U.S. Patent Application No 2004/0215964), further in view of Deindl (U.S. Patent No. 6,076,162).

Without conceding the correctness of the rejections and in order to advance prosecution on the merits, Applicants have amended claims 1 and 13 to define more particularly the subject matter sought to be patented, and have canceled claims 3 and 16. In addition, Applicants have amended claims 22-25 to recite a "microcircuit" rather than a "method." The amendments add no new matter. Support for the amendments appear in the specification as originally filed, for example, in originally presented claims 1 and 13, and at Figures 1-4 and the accompanying textual description.

Applicants submit that claim 1, as amended is directed to subject matter that is patentable over Ishiguro, Barlow, and Deindl. For example, none of references of record (Ishiguro, Barlow, or Deindl) disclose or suggest, as recited in Applicants' claim 1 as amended, a step of storing a certificates table containing a digest form of at least one public key in a memory in the microcircuit, wherein the public key is inserted into the certificates table by a step that comprises inserting, in the certificates table, a pointer to the digest form of the public key of the certification entity that issued the certificate of the public key, so as to define a certification tree in combination with the inserted digest form of the public key. In addition, none of the references of record disclose or suggest the claimed steps of "calculating a digest form of the

received public key," and "searching for the calculated digest form of the public key in the microcircuit's certificates table, at a location at which the inserted pointer points."

The Examiner relies upon Deindle as disclosing the claimed use of a "digest form" of a public key. (Office Action, at pages 4 and 27.) The Office Action in particular states that it is the "certificate key" (sic: "certifying key" or "certification key") from Deindle that the Examiner contends to be the claimed "digest form of at least one public key." (Office Action, at page 4.) Applicants disagree. Deindle makes absolutely clear that its certifying, or certification, key that is stored in, and searched for in, the chipcard is the public key. Indeed, Deidle states that "[t]his certification key is the public key of the stated pair of keys and must be authorized to release the certification and must, itself, already been certified." (Col. 5, lines 62-65.) As one of skill in the art would understand, a "digest form" of a public key is less than the entire public key. This is exemplified from the example embodiments disclosed in Applicants' specification, where it is described that a hashing function is used, for example, to create a digest form of the public key, and this hashed "digest form" of the public key is stored in the microcircuit, rather than the public key itself. (See Applicants' specification at page 7, lines 18-22.) As such, it is clear that the claimed "digest form" of a public key is less than the full information of the public key itself. This, again, is not the case with the "certificate key" disclosed in Deindl.

In addition, because in Deindl there is no storage of a "digest form" of a public key stored in the microcircuit, Deindl also does not disclose or suggest, as recited in claim 1, a phase of checking a digital signature that comprises searching in the microcircuit's certificates table for a calculated "digest form" of a public key. Moreover, Deindl does not disclose or suggest searching for the calculated "digest form" of the public key at a "location at which the inserted pointer points," as recited in claim 1.

While Deindl does indeed describe the use of hash algorithms, the use of hash algorithms in Deindl is limited to cryptographic procedures of data encryption/description (e.g., col. 4, lines 16-33). Deindl does not disclose or suggest, as Applicants are claiming, using those hash algorithms to generate a digest form of a public key, storing that digest form of the public key on the chipcard, and performing the check of a digital signature in the manner recited in Applicants' claim 1. Again, Deindl discloses storing the public key itself in the chipcard.

In addition, Applicants also disagree that Barlow discloses the use of a certification tree, which previously was recited in Applicants' claim 3, but now is recited in Applicants' claim 1. Applicants respectfully disagree. Barlow teaches the certificates of the public keys stored on the microcircuit are not linked with each other (see, for example [0045], [0056], and [0071]). Barlow only mentions an external certifying authority adapted to certify public keys generated by the chipcard, but does not suggest or disclose any certification tree defined in a certificates table as recited in Applicants' amended claim 1. The certification tree characteristic is neither disclosed in the Ishiguro reference nor the Deindl reference.

Because Ishguro, Barlow, and Deindl, alone or in combination, fail to teach or suggest each and every feature of claim1, they cannot possibly render claim 1 obvious. Applicants therefore respectfully request that the Examiner withdraw the rejections and allow claim 1.

Claim 13 contains features that are similar, but not identical to the features described above for claim1, and is therefore allowable for at least the reasons given for claim1. Applicants therefore respectfully request that the Examiner withdraw the rejections and allow claim 13.

Claims 2, 4-12, 15, and 17-25 are variously dependent on claims 1 or 13 and are therefore allowable for at least the reasons given for claims 1 and 13. Applicants therefore respectfully request that the Examiner withdraw the rejection and allow claims 2, 4-12, 15, and 17-25.

CONCLUSION

Applicants submit that claims 1-2, 4-13, 15 and 17-25 are in condition for allowance, and respectfully request that a notice of allowance be issued.

It is believed that all of the pending issues have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally nothing in this reply should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this reply, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicants have requested separately a Petition for Extension of Time, and have authorized the payment of the fee for such Extension of time from deposit account 06-1050. If any other charges or credits are due, please apply any such charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: Oct. 19, 2009

/Stephen R. Schaefer, Reg. No. 37,927/
Stephen R. Schaefer
Reg. No. 37,927

Fish & Richardson P.C.
3200 RBC Plaza
60 South Sixth Street
Minneapolis, Minnesota 55402
Telephone: (612) 335-5070
Facsimile: (877) 769-7945